Demo: UI Based Attacks in WebXR

Chandrika Mukherjee, Reham Mohamed Aburas, Arjun Arunasalam, Habiba Farrukh, and Z. Berkay Celik

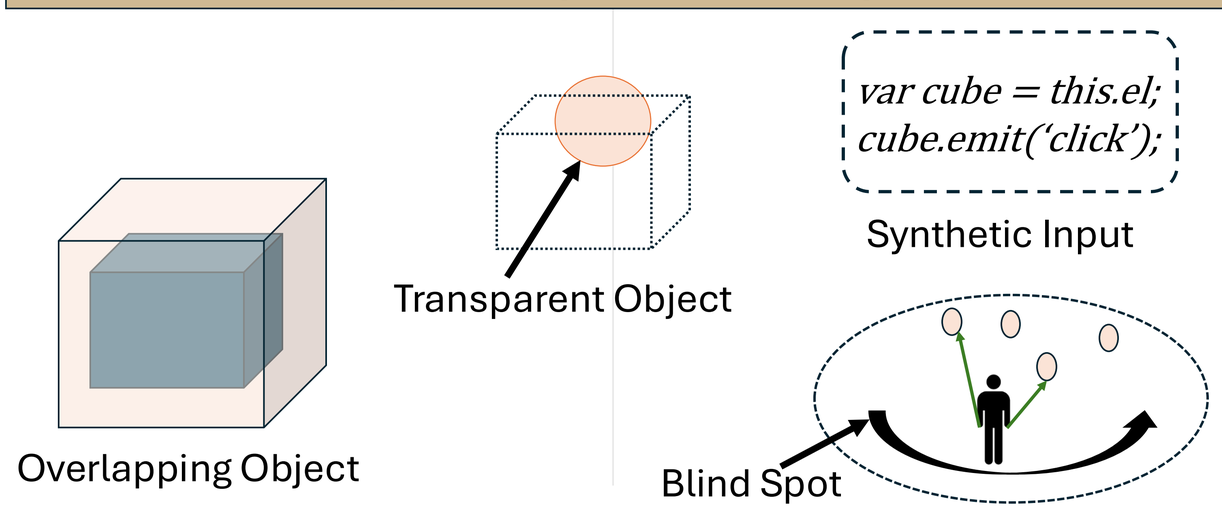
PURDUE UNIVERSITY · AUS American University of Sharjah · UCI University of California, Irvine

ACM MobiSys2025

Background & Motivation

- **WebXR** enables immersive AR/VR experiences through browsers on head-mounted displays (HMDs).
- **Security-sensitive UI properties** (e.g., transparency, synthetic input) can be exploited for UI-based attacks [1,2,3].
- Unlike the standard web, **WebXR lacks <iframe>** like element that separates execution of different origins.
- Third-party entities, such as advertisements, **share the same scene** as other objects within the publisher's WebXR site.
- Our prior work [3] identifies **five novel UI-based attacks** in WebXR that exploit the advertising ecosystem.
- This demo integrates these attacks in a **gaming environment** into distinct interactive scenarios to show their effectiveness.

Example Of Exploitable UI Properties



Beneficial Use Cases

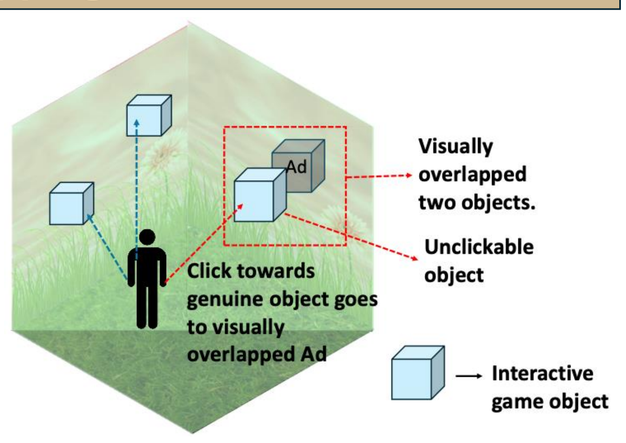
- Transparency creates visual effects (e.g., depth, flowing water, shattering glasses).
- Same place overlapping objects create complex scene with intricate architecture.
- Synthetic input can be used for dynamic object interaction.
- Auxiliary screen can be used by developers for debugging.
- Programmatic screenshot capture can be used for automated testing, media sharing etc.
- Gaze-fusing override provides faster and more precise interaction.

UI Based Attacks

- These UI properties can be exploited in WebXR advertising ecosystem.
- Advertiser, ad service provider, and developer - any of these entities can act as an adversary.
- These attacks compromise user autonomy, leading to data theft and malware downloads onto the user's system.
- Additionally, these attacks can cause financial or reputational damage to the ad stakeholders.

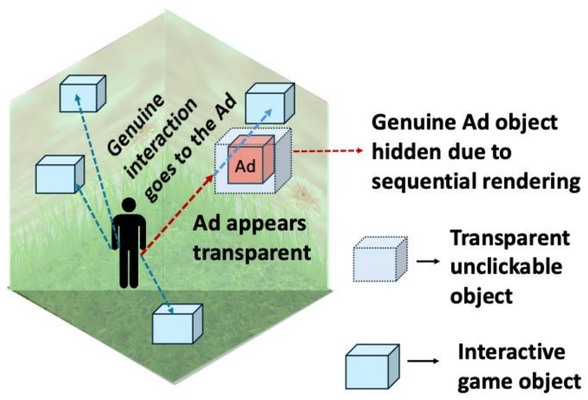
Visual Overlapping Attack

- **Exploited properties** - Synthetic input, click received by first clickable object
- **Adversary** – Developer
- **Goal** – Revenue from ad clicks
- **Malicious Impact on** – User, advertiser



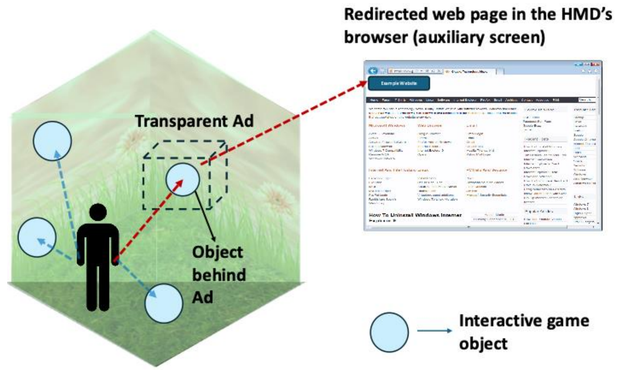
Sequential Rendering Attack

- **Exploited properties** – Transparency, same space overlapping objects, synthetic input, sequential rendering, click received by first clickable object
- **Adversary** – Developer
- **Goal** - Revenue from ad clicks
- **Malicious Impact on** – User, advertiser



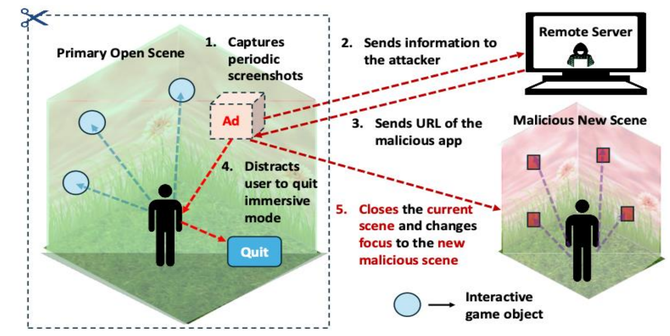
Malvertising Attack

- **Exploited properties** – Lack of iframe, transparency, scene entry/exit detection, click received by first clickable object, auxiliary screen
- **Adversary** – Advertiser
- **Goal** – Increase SEO ranking or video views
- **Malicious Impact on** – User, developer, ad service provider



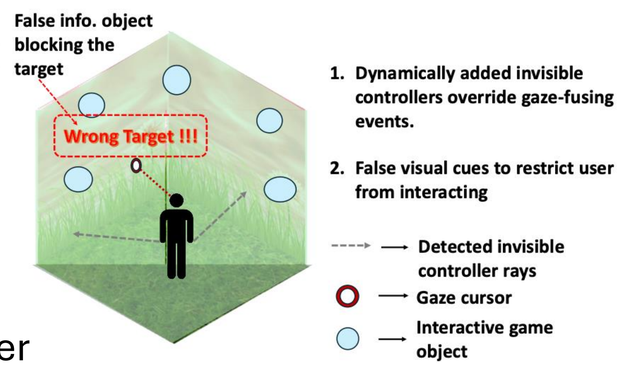
GUI Switch Attack

- **Exploited properties** – Lack of iframe, scene entry/exit detection, capturing programmatic screenshot
- **Adversary** – Advertiser
- **Goal** – Extracts user's private information
- **Malicious Impact on** – User



DoS Through Overriding Attack

- **Exploited properties** – Lack of iframe, transparency, gaze-fusing override
- **Adversary** – Competitive ad service provider
- **Goal** – Restrict user's intended action
- **Malicious Impact on** – User, other ad service provider, advertiser



Takeaways & Future Directions

- The UI properties can be exploited knowing or unknowingly, raising the risk for UI based attacks with integration of third-party objects.
- Critical need for user-centered design approaches that maintain action awareness in immersive environments.
- To investigate whether developers encounter challenges in integrating third-party objects into immersive scenes, and to identify those challenges.

Acknowledgements

This work was partially supported by NSF grants CNS-2144645 and IIS-2229876. The findings and recommendations in this work are those of the authors and do not necessarily represent the views of the NSF.

Survey QR Code

Please scan this QR code to participate in our follow-up survey.

References

[1] Hyunjoo Lee, Jiyeon Lee, Daejun Kim, Suman Jana, Insik Shin, and Sooel Son. 2021. AdCube: WebVR Ad Fraud and Practical Confinement of Third-Party Ads. In USENIX Security.

[2] Kaiming Cheng, Arkaprabha Bhattacharya, Michelle Lin, Jaewook Lee, Aroosh Kumar, Jeffery F. Tian, Tadayoshi Kohno, and Franziska Roesner. 2024. When the User Is Inside the User Interface: An Empirical Study of UI Security Properties in Augmented Reality. In USENIX Security.

[3] Chandrika Mukherjee, Reham Mohamed, Arjun Arunasalam, Habiba Farrukh, and Z. Berkay Celik. 2025. Shadowed Realities: An Investigation of UI Attacks in WebXR. In USENIX Security.